CLAIMS

We claim:

1. A method for detecting computer hacker denial of service attacks, comprising the steps of:

issuing a bit mapped challenge in response to a login request from a requester of services; and

responsive to an incorrect response to said challenge, placing said requester in a state of limited service.

2. The method of claim 1, further comprising the steps of:

filtering out to said state of limited service iterative connection requests from a network address of a hacker device.

3. The method of claim 1, further comprising the step of:

responsive to speed, latency and average queuing

network delay of connection requests, detecting and placing in a state of limited service repetitive login requests from a hacker device.

4. The method of claim 3, further comprising the steps of:

determining from said speed, latency and average queuing network delay a time-out value; and

detecting as a request from a hacker device a request that does not complete within said time-out value.

5. The method of claim 1, further comprising the steps of:

issuing further challenges to subsequent requests for service from said requester and selectively responding to successful responses by continuing service at the same or improved level and to unsuccessful responses by further reduction or complete denial of service.

6. The method of claim 1, further comprising the steps of:

periodically issuing said challenges throughout connection to a requester successfully responding.

7. The method of claim 1, comprising the step of issuing said bit-mapped challenge as logon image from which a user must select or enter a response.

8. The method of claim 7, further comprising the step of occasionally shifting the input area for a valid response to said challenge.

9. The method of claim 1, further comprising the step of slowing acceptance from and response to systems in a degraded service category.

10. The method of claim 1, further comprising the step of counterattacking by executing a denial of service response to attacking systems.

11. A method for detecting computer hacker denial of service attacks, comprising the steps of:

executing a challenge-response login procedure and a network probing test frame transmission and analysis procedure to detect a hacker denial of service attack; and

responsive to detecting said denial of service attack,

placing said hacker in a lower level of service state.

12. A method for detecting computer hacker denial of service attacks, comprising the steps of:

selecting sending and receiving probative test packets through a network;

responsive to said packets, determining network evaluation parameters for said network; and

responsive to said network evaluation parameters, determining presence of network denial of service attacks.

13. The method of claim 12, said network evaluation parameters including response time and throughput characteristics of said network.

14. The method of claim 13, said throughput characteristics including capacity, utilization, and performance.

15. The method of claim 13, further comprising the steps of executing a challenge-response procedure to discourage and repel said attacks.

16. The method of claim 14, further comprising the steps of:

determining a latency and speed fingerprint of an offending device;

responsive to said fingerprint, operating a router filtering system to reject packets from said offending device.

17. The method of claim 16, said fingerprint comprising a rhythm of transmissions of discrete, burst, and stream packets.

18. A system for detecting and responding to denial of service attacks, comprising:

a test station for identifying a zombie source of said denial of service attack;

a low quality server for serving said zombie source; and

a high quality server for serving legitimate sources of request for services.

19. The system of claim 18, further comprising:

a load balance server for directing said zombie source to said low quality server.

20. The system of claim 19, said zombie source being an a server addressable on an Internet containing trojan-horse code.

21. The system of claim 18, said test station performing testing by use of ICMP pings to identify said zombie source.

22. The system of claim 21, said test station further for determining patterns of traffic generated by well-known attack scripts for subsequent use in identifying said zombie source.

23. The system of claim 21, said test station further for determining a timeout value for completion of a login request for freeing control blocks responsive to a login request which does not complete within said timeout value.

24. A probative test and analysis method for detecting and responding to denial of service attacks on a network resource, comprising the steps of:

creating a template of attack patterns;

determining historical, current, and predicted states of said network for each of a plurality of types of network traffic;

responsive to said attack patterns, determining if a spike in network traffic is a distributed denial of service attack and, if so, determining its source; and

denying full service to sources associated with said service attack.

25. The method of claim 24, further comprising the steps of:

determining unique speed and latency network attachment characteristics of devices attempting to connect to said network resource; and

responsive to detection of an abusive behavior from a said device, responding to subsequent requests for service from said device by denying said full service to said device.

26. A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for detecting computer hacker denial of service attacks, said method steps comprising:

issuing a bit mapped challenge in response to a login request from a requester of services; and

responsive to an incorrect response to said challenge, placing said requester in a state of limited service.

27. A computer program product or computer program element for detecting computer hacker denial of service attacks, according to method steps comprising:

issuing a bit mapped challenge in response to a login request from a requester of services; and

responsive to an incorrect response to said challenge, placing said requester in a state of limited service.

28. A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for detecting computer

hacker denial of service attacks, said method steps comprising:

selecting sending and receiving probative test packets through a network;

responsive to said packets, determining network evaluation parameters for said network;

responsive to said network evaluation parameters, determining presence of network denial of service attacks; and

denying full service to sources associated with said denial of service attack.

29. A method for detecting distributed denial of service attacks, including the steps of:

executing a network probing test frame transmission and analysis procedure to detect a hacker denial of service attack; and

responsive to detecting a denial of service attack, placing said hacker in a state of lower level of

service.

30. A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for detecting computer hacker denial of service attacks, said method steps comprising:

executing a network probing test frame transmission and analysis procedure to detect a hacker denial of service attack; and

responsive to detecting a denial of service attack, placing said hacker in a state of lower level of service.